Available online at www.sciencedirect.com

SCIENCE DIRECT®

Government Information Quarterly 21 (2004) 399–405

Government Information Quarterly

Do you know where your information is in the homeland security era?[☆]

Jeffrey W. Seifert*, Harold C. Relyea

Congressional Research Service, Library of Congress, Washington, DC 20540-7450, USA

Available online 28 October 2004

Abstract

Why should we care about our information? As we enter the era of homeland security, one can see a new premium being placed on the role of information to fight terrorism while the policies related to government information practices are in a state of flux. Exactly how these policies are evolving is not always clear. Yet, the decisions being made now will likely have a lasting impact for years to come. In an attempt to better understand dynamics underlying these changes, a number of questions regarding the use, control, and protection of personal and public information are posed in this introduction to the symposium issue. We also review some of the major themes examined in greater detail by the contributors to the symposium. These issues include the role of e-government in homeland security, the emphasis on information sharing, the emergence of new information classification categories, the growth of data mining, and the eroding sense of privacy. While a number of reasons can be offered to justify one policy alternative over another, we conclude that the importance of these issues suggests that they are best debated and implemented during a time not under duress when decisions made in the heat of the moment can lead to unintended consequences.
Published by Elsevier Inc.

[☆] The views expressed in this article are those of the authors and do not necessarily reflect the position of the Library of Congress or the Congressional Research Service.

* Corresponding author. Fax: +1 202 707 7000.
E-mail address: jseifert@crs.loc.gov (J.W. Seifert).

0740-624X/$ - see front matter. Published by Elsevier Inc.
doi:10.1016/j.giq.2004.08.001

1. Introduction

We are entering an era that, for the forseeable future, will be dominated by homeland security. While the concept of homeland security itself remains somewhat ambiguous,[1] meaning different things to different people, concerns about homeland security are affecting issues across the policy agenda. As happened with the similarly uncertain national security concept with the onset of the Cold War, a variety of issues regarding public health, critical infrastructure, commerce, agriculture, education, and transportation, to name a few, have all been recast, to varying degrees, in the context of homeland security. Issues related to technology, information, and electronic government (e-government) are also no exception. However, the vagueness surrounding the concept of homeland security is being carried over to the other issues it is being applied to. One specific area of relevance to this journal where this problem is particularly acute involves the information practices of the federal government.

It is not surprising that technology plays a significant role in homeland security. The rapid growth of the Internet and the dot-com boom of the 1990s helped drive a new wave of technology innovation and investment in the private sector. E-commerce took root, knowledge workers flourished, and companies sought new ways to harness their information assets. Toward the end of the dot-com boom, and increasing with the dot-bomb bust (when the federal government became one of the few entities to have increases in information technology spending), the same forces that attempted to transform the private sector began to focus in earnest on the public sector. E-government applications, more of a concept than a reality in the 1990s, rapidly proliferated in the past few years and have begun to mature as governments at all levels have attempted to transform their processes in the name of efficiency, improved services, and better government. Similar to our Cold War support for weapons technology, current enthusiasm in technology is naturally embodied in homeland security efforts, which are attempting to further transform government processes and ensure security with a sense of urgency. However, while technology is a critical component of homeland security, the technology itself is merely a tool to support the core substance of homeland security, namely, information.

In many respects, the Department of Homeland Security (DHS) came into being and functions as arguably the first virtual agency in the e-government era. While one of the largest departments in the federal government, with an estimated 180,000 employees from twenty-two agencies, only a relatively small fraction of these employees (approximately 18,000) are currently located in Washington, DC.[2] The overwhelming majority of the department's personnel are spread out across the country, guarding border crossings, inspecting shipments, monitoring terrorist networks, analyzing data, and carrying out other responsibilities. While still being developed, the longer-term goal is to create a network that will allow DHS to capitalize on its knowledge assets to facilitate information sharing and enhanced communication. This suggests that officials have high expectations for the quality of the information, and their ability to use the information to enhance security. Organizationally, this will involve breaking down the "stovepipes" that have previously separated the department's components and developing an encompassing organizational culture that promotes cooperation and information sharing. Technologically, this will involve integrating existing systems and infrastructures, while simultaneously infusing new technologies as they become available, through the development of an enterprise architecture.[3] Administratively, this will involve changing some of the policies and regulations pertaining to the collection, use, and dissemination of information.

Taking a broader view, we see that policies related to government information practices are in a state of flux. While exactly how they are evolving is not always clear, what is evident is that many of these changes are being driven largely by concerns to improve security, or, at the least, to not allow information to become a vulnerability that can be exploited by terrorists. It would then appear that the implicit goal behind these efforts is to shift control over information more towards the federal government, and its contractors, while at the same time increasing the degree of latitude these actors have to use the information for different purposes. Depending upon the final outcome, these changes could significantly alter the relationship between citizens and government in the United States, which, in turn, raises a number of questions to consider when formulating new policies.

2. Do you know where your information is?

2.1. Why should we care about our information?

Those who are not students of government information policy may wonder why one should care about these issues at all. Some suggest that “it is only information,” and that is cannot hurt anyone. Others claim that, as long as they do not do anything illegal or “wrong,” then there is nothing to fear. However, if information is the currency of the e-government/homeland security era, then the reasons to care are many. Privacy, once defined by Supreme Court Justice Louis Brandeis in the *Harvard Law Review* as “the right to be let alone,”[4] is perhaps the most compelling reason. Privacy, not to be confused with anonymity, suggests individuals have some modicum of control over information about themselves and their actions. Once lost, privacy cannot be effectively regained. Moreover, the accumulation of information over time presents the opportunity for repeated and more invasive intrusions into one’s privacy. A second reason involves the accuracy of information. Inaccurate information can affect a multitude of decisions, unbeknownst to the affected individual, until after the fact. Mistaken identities can lead to false arrests. Inaccurate credit reporting can affect an individual’s ability to obtain a loan or even a job. Sloppy medical record keeping can lead to inappropriate medical care. These mistakes are compounded by a third reason directly related to accuracy: the apparent faith in information that seems to be exhibited by the public and private sectors alike. The decreasing cost of computers and storage, coupled with the increased availability of usable data, has led many organizations to try to capitalize on these resources and automate a number of functions previously handled by people. The consequence is that there can be fewer opportunities to prevent decisions made based on incorrect data, and fewer opportunities to correct the data errors. Taken as a whole, information about ourselves can reflect on us both positively and negatively, frequently without our knowledge, in an increasing number of circumstances, suggesting we should care about our information.

2.2. What should we use our information for?

This question is relevant both for the original justification for collecting the information, as well as for potential reuse of the data for other purposes later. Authorized use of information is an issue that has loomed large in discussions of homeland security information practices. Data mining is already fairly widespread throughout the federal government for purposes such as identifying fraud, improving program management, and analyzing scientific management. Computer matching by federal agencies has traditionally been closely regulated, requiring public notice and adherence to various privacy rules. However, to facilitate efforts to track down and capture potential and known terrorists, some U.S. laws, including the USA PATRIOT Act, have been passed or revised to reduce the barriers between domestic and foreign security operations and facilitate information sharing. Barriers may be further reduced as new applications are developed and used for purposes in addition to those originally intended. One such example is the Computer Assisted Passenger Prescreening System (CAPPS II). CAPPS II is being created to enhance airline security with the intent of catching foreign terrorists, but the Transportation Security Administration has suggested it could also be used for domestic law enforcement purposes. Further questions are raised by government use of data held by the private sector. Some observers have suggested this is a means to gain access to information the federal government may be otherwise barred from collecting. Likewise, questions have been raised regarding whether public sector data should be sold to the private sector. Some states sell information about their citizens, such as data collected through motor vehicle administrations. Concerns about the use of information also extend to the international level, whereby countries with more stringent privacy laws (data protection) have been reluctant to share data with the United States. In any event, it appears likely that we will see further attempts to capitalize on existing data pools for new purposes.

2.3. How do we protect our information?

Information protection involves both policy and technological solutions. It also involves striking a balance between protection and access. Classification schemes are at the center of the policy solutions. In the U.S., there is some debate over the alleged tendency of government officials to classify too much information, as well to refrain from declassifying information long after it is eligible to be released to the public. While the overuse of classification can be troublesome, so can the use of ill-defined protection schemes. Reliance on ambiguous and undefined security labels, such as “sensitive but unclassified,” that exist outside a recognized system of classification raise questions about the legitimate use of information, as well as the legitimacy of such a label. While protecting sensitive data is critical to security, the lack of a clear system of protection can unnecessarily raise red flags about the activity and data in question, and reduce the transparency of government. In the case of technological solutions, information security represents an evolving problem with no definitive endpoint. The lack of appropriate security precautions can contribute to a decline in the confidence of an agency to properly handle data, not to mention undermine the project itself if sensitive data is involved. However, good information security practices require continual vigilance, regular testing, and can be costly. Data protection also involves protection of the infrastructures used to access and transmit the data, requiring agencies to reinforce their networks and invest in redundant systems to maintain continuity of operations and backup copies of their data.

2.4. Where do we put our information?

This is a question that, in the government context, citizens rarely have control over, but should be aware of all the same. Where our information is located, and where it gets moved to, is directly related to both the use and control of information. It is also pertinent to the issue of access to public documents. Sometimes attempts may be made to combine information from different sources into a centralized database. However, this may raise concerns about whether the data could be used improperly, as well as security concerns, by creating a rich target for hackers. Sometimes distributed databases may be used to enable information sharing and data mining, while allowing the data owners to retain greater control over who has access to the data and how it is used. In the case of public documents, many are now appearing only in electronic form on Web sites and other sources. This raises questions about the appropriate distribution and archiving of information.

2.5. When do we lose control over our information?

Control over information is a double-edged sword. On the one hand, most people want to control access to their personal information. On the other hand, many civil libertarians would like to see the government exercise less control over what information is made publicly available. Digital information can be replicated and distributed infinitely without a loss of quality or value. Digital information is also easy to transmit and store inexpensively. Arguably, we lose control over our information immediately after we give it to someone, which is why it is critical not only to have good information practices and laws in place regarding information already collected, but also to be vigilant about the unnecessary collection of information. Information in databases can be easily transferred from one network to another. Public documents posted on a Web site can be replicated and mirrored on the Internet. In the case of personal information, one approach to stemming the proliferation of one's information is to be more judicious in providing information to others whenever possible. The refusal to provide information can result in the denial of services or products. However, there may be times when the costs associated with providing information outweigh the benefits received by doing so. In the case of public information, careful thought needs to be given to what types of information are truly sensitive and those which are not. Is the concern about a specific piece of information, or the ability to combine disparate pieces of information? Is there a way to balance the public's right to know with security concerns?

In different contexts, the contributors to this symposium attempt to address these questions while raising additional ones. Elaine Halchin evaluates how the federal government's war on terrorism has affected, and is affected by, e-government, which can be both a strength and a vulnerability. Harold C. Relyea provides a nuanced analysis of how the rapid growth of information sharing promoted by the Homeland Security Act appears to have outpaced its regulatory framework, leaving many important policy considerations open to interpretation. In a related vein, Lotte E. Feinberg examines how the proliferation of new categories of records, such as "sensitive but unclassified," "for official use only," and "critical infrastructure information," has the potential to allow large amounts of information to remain out of reach of the traditional declassification and Freedom of Information Act (FOIA) processes, renewing a conflict between the need for secrecy versus the public's right of access. Jeffrey W. Seifert examines how the growth of homeland security data mining initiatives, such as the Computer-Assisted Passenger Prescreening System (CAPPS II) and the Multistate Anti-Terrorism Information Exchange (MATRIX) may not deliver their anticipated results due to limitations such as data quality, mission creep, and privacy concerns. Priscilla M. Regan assesses how the increased ability of the federal government to collect information from different sectors, combined with lower legal standards required to act on this information, has affected privacy and due process safeguards. While these articles capture the fluid nature of the ongoing changes in the federal information practices environment, they represent a snapshot at the time of their writing. Consequently, future assessments will likely be merited.

3. Conclusion

In many respects, this symposium issue is meant to update and continue the policy discussion started in an earlier symposium issue.[5] The earlier symposium reflected the initial reactions of the policy community to information issues very shortly after the September 11, 2001, terrorist attacks. Since then, a number of significant changes have taken place. Electronic government is becoming more integrated and embedded into government operations. The Department of Homeland Security has been created. There is a strong emphasis on government sharing of many types of information, including critical infrastructure information, terrorist watch lists, and travel information. There have been sweeps of government Web sites to identify information that could be of potential use to terrorists. There is a greater interest in making some types of information exempt from FOIA requirements. Dataveillance is on the rise. Security concerns seem to pervade most issues.

Nearly three years after the terrorist attacks, we are approaching a critical juncture. The decisions being made now will establish both the technological and policy infrastructures for homeland security, and are likely to have a lasting impact for many years to come. In the words of Benjamin Franklin, quoted in the *Historical Review of Pennsylvania* (1759): "Those that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.” Currently, many of the rules governing the information practices discussed in this issue are shown to be vague and/or evolving, and in some cases, non-existent. This suggests a need for clear rules and procedures, which are best debated and implemented during a time not under duress when decisions made in the heat of the moment can lead to unintended consequences.

Notes and References

1. See Relyea, H. C. (2002). Homeland security and information. *Government Information Quarterly, 19,* 213–223.
2. See Kaufmann, T. (2002, December 2). OPM promises homeland security personnel system by June. *Federal Times, 1,* 5;
   Lee, C. (2002, December 9). OPM begin sorting security personnel. *Washington Post,* A21.
3. An enterprise architecture serves as a blueprint of the business operations of an organization and the technologies needed to carry out these functions. Ideally, it is designed to be comprehensive and scalable to account for future growth needs. See U.S. General Accounting Office. (2003, April). *Information technology: A framework for assessing and improving enterprise architecture management (version 1.1)*. http://www.gao.gov/new.items/d03584g.pdf
4. Warren, S. D., & Brandeis, L. D. (1890, December 15). The right to privacy. *Harvard Law Review, 4,* 193–220.
5. Symposium issue: Issues in homeland security and information. (2002). *Government Information Quarterly, 19*.